IDC TECHNOLOGY SPOTLIGHT

The Imperative of Merging Identity with Software-Defined Networks

August 2016

Adapted from *Cloud and Drive for WAN Efficiencies Power Move to SD-WAN* by Brad Casemore, Rohit Mehra, and Nav Chander, IDC #US41101416

Sponsored by Tempered Networks

This paper examines the growing need to conjoin networking and security through emerging technologies that provide network virtualization for digital transformation initiatives while addressing the need for pervasive threat mitigation. It also looks at the role of Tempered Networks, whose identity-defined networking (IDN) platform is designed to deliver secure overlay networking (or secure software-defined networking [SDN]), which affords enterprise IT a means of achieving identity assurance and granular network microsegmentation extending from the datacenter network to a variety of WAN endpoints.

Introduction

Enterprise IT today is defined by unprecedented challenges, most of which have significant architectural, operational, and security implications for network infrastructure.

For example, enterprises worldwide have made digital transformation a critical business priority. IDC defines digital transformation as the application of 3rd Platform technologies — cloud, mobility, data analytics, and social business — to fundamentally change the nature and value of business models, business processes, and products and services.

What's more, enterprises recognize that digital transformation is an imperative, not an option. Eschewing the need for digital transformation often results in falling behind the competition, loss of revenue and market share, and even business irrelevance. Indeed, IDC predicts that by 2018, one-third of the top 20 market leaders in most industries will be significantly disrupted by new competitors that use the 3rd Platform to create new services and business models.

The 3rd Platform, on which digital transformation depends, has become an undeniable technological foundation for business process improvement and also for improved business outcomes. Cloud and mobility have been key pillars of the 3rd Platform and have generated opportunities as well as challenges for enterprise customers as well as for the vendors that serve them.

As a result of the proliferation of endpoints and the increasing adoption of cloud computing, enterprises are rethinking and rearchitecting their networks. The requirements associated with cloud computing have already reverberated through datacenter networking. With cloud as the driver, SDN arose as an architectural approach that provides the network with the agility and responsiveness previously lacking — through automated provisioning, programmatic management, and integration with cloud orchestration platforms. Now, the focus is turning to how the campus and the WAN must be modified to accommodate the dynamic requirements of cloud computing. In fact, the WAN is an increasingly critical foundational element in the realization of hybrid cloud for enterprises worldwide.

Enterprises adopting hybrid cloud must give careful consideration to a WAN strategy that offers the same sort of business agility, operational efficiencies, and security that they seek to derive from SDN in the enterprise datacenter and the campus.

Enter SD-WAN

SD-WAN started gaining mindshare in 2015 as a key subset of the overall SDN market. IDC predicts SD-WAN revenue will ramp up strongly in 2016 across a broad range of vertical markets, including retail, banking, financial services, and healthcare. IDC believes that SD-WAN's value proposition — predicated on the growth of cloud computing, the need for simplified VPN capabilities, and the business imperative of reducing MPLS costs — will be compelling for a growing number of enterprise customers seeking to provide cost-effective cloud-era networking to branch offices and remote sites.

With the combination of cloud computing, mobile, and the Internet of Things (IoT), the tasks of connecting and securing the assets of any organization with existing solutions have become exponentially more difficult. Perimeter security, applicable to the needs of client/server computing and the 2nd Platform, is outmoded and unable to address the new requirements associated with digital transformation on the 3rd Platform.

Unifying Security Across All SDN

Increasingly, networking and security will have to become seamlessly interconnected rather than deployed and managed separately, including WANs that are software defined. The "secure SDN" might be achieved through different means, but one emerging alternative involves bringing seamless trust through cryptographic identities (CIDs) to SDN. Securing an SD-WAN would involve pushing security policies as close to endpoints as possible and leveraging those routable and unique CIDs for location instead of an IP address. Doing so would enable provisioning of network and security services quickly and easily, without the need for advanced IT skills or personnel and the overhead associated with complex firewall rules, ACLs, and a sprawling number of VLANs. In addition, enterprises need to be able to leverage connectivity beyond the WAN, including cellular, WiFi, and satellite networks.

A new approach is required to create the trust and pervasive security required for IoT, mobility, and public cloud. In the past, trusted (whitelisted) devices and subscribers were connected to a trusted network with complicated equipment and potentially costly networking services. Fortunately, now they can be connected in a simplified manner as a result of recent innovations in networking and orchestration.

Benefits

A principal benefit of this approach to "secure SDN" involves the enablement of a network security posture that is simple to implement and easy to maintain and provides for agility and flexibility in support of key business imperatives such as digital transformation and IoT.

To be sure, such a system allows IT staff to rapidly provision encrypted overlay networks that can easily ride atop any existing underlay network or network infrastructure. As a result of using an orchestration server that abstracts the complexities associated with traditional approaches, there is no requirement to implement and manage firewall rules, ACLs, VLANs, or software agents. There is also no need to manage encryption keys. As a result, the architectural simplicity helps reduce both complexity and operational costs.

These benefits can extend across multitenant datacenter networks, campus networks, and WANs, including branch offices that increasingly require open APIs and improved flexibility to support dynamic traffic flows and to mitigate latency. What's more, the capabilities associated with these benefits encompass secure management and orchestration of both east-west and north-south traffic flows.

Furthermore, this approach can improve an enterprise's risk profile and security posture in several respects. Through "cloaking," for example, which makes the IP footprint of endpoints invisible, it can mitigate the threat exposure of servers, hosts, and services, thereby reducing the overall number of attack vectors. This reduction translates directly into a simplification of the

network security architecture — reducing the number of firewall rules, simplifying the firewall rules that are still required, simplifying and streamlining network routes, reducing the range of traffic requiring inspection, and mitigating the impact of malware through proactive and remedial microsegmentation.

The simplified nature of the approach also carries a notable operational benefit. During a period in which a significant skills gap exists in enterprise IT departments, which are struggling to adapt to the needs of cloud computing and to the automation-related requirements of SDN, any technology that does not entail meaningful IT skills upgrades carries added utility and practical business value.

Considering Tempered Networks

Tempered Networks' Identity-Defined Networking (IDN) platform enables enterprise customers to seamlessly secure network segments and to transform vulnerable IP-enabled devices into hardened, invisible assets. IDN is a fabric-based architecture that unshackles the network from the problems associated with IP addressing across networks by creating a global IP namespace. The platform is designed to deliver secure overlay networking (or secure SDN), affording enterprise IT a means of achieving identity assurance and granular network microsegmentation from the datacenter network to a variety of WAN endpoints.

Tempered leverages the Host Identity Protocol (HIP), an Internet Engineering Task Force (IETF) standard that uses cryptographic identity instead of IP addresses to automate and manage identities on a network.

HIP provides an alternative key-exchange capability for the IPsec protocol, enabling transparent and legacy-compatible security for all TCP/IP applications. HIP introduces the concept of an identifier-locator split that effectively decouples the dual role of IP addresses providing host identity and topological location on the Internet. Instead, under HIP, hosts are identified using strong cryptographic identities in the form of 2,048-bit RSA public keys. The locator remains an IPv4 or IPv6 address, but the identity is not tied to the host IP address. Hosts can change their IP location on demand and without disruption while retaining their strong cryptographic identity.

As a result, HIP remains compatible with IPv4 and IPv6 applications, utilizing customized IPsec tunneling for confidentiality, authentication, and integrity of the network applications. HIP provides strong security properties by relying on formal verification of its state machine describing each step of protocol operation.

Because hosts and network devices can use unspoofable CIDs rather than transient IP addresses for identification, IT professionals can easily implement functionality such as host and network mobility, single sign-on, and multihoming. The Tempered Networks IDN platform features tight integration between the Conductor — an orchestrator or controller with a management console/UI that allows for management of groups of devices for large-scale deployments — and HIP services that provide a gateway for trusted network traffic between protected (explicitly whitelisted) endpoints and devices.

HIP services are available on a variety of platforms, either in the cloud or on hardware or virtual HIPswitch appliances, and also include HIPapp client-side applications. HIP services are topology and protocol agnostic and can provide connectivity over any mix of wired Ethernet, satellite, or cellular communications. Various models are available for datacenter or industrial environments, which might require hardening for extreme conditions.

In deploying HIPswitches, an enterprise effectively builds a private overlay network between devices. The overlay network is completely agnostic to and isolated from the "underlay" network, meaning it can leverage existing enterprise investments in network infrastructure. Tempered Networks provides a global IP namespace that enables instant movement of endpoints and systems across hybrid networks, without requiring any IP routing changes. Its encrypted fabric ensures that all whitelisted endpoints and machines will be able to find trusted endpoints or systems securely, regardless of where they sit or what IP address they are using.

For example, a customer could take a physical SQL Server and move it to a virtual SQL Server, and then move it to AWS, without ever having to change its IP address. The SQL Server's behavior stays the same — regardless of the network or addressing scheme employed by that network.

The Tempered IDN platform's approach is designed to reduce network complexity while improving an enterprise's security posture. By reducing the visible attack surface, security administrators gain the ability to automatically reduce much of the noise that plagues most enterprise networks today. Looking at several recent high-profile breaches, we note that many of the infections were detected by a security device in the breached network, but because of the sheer number of alerts inundating the security team, each attack was undiscovered until well after the breach had occurred and data was lost.

Another benefit of the IDN platform is its ability to simplify and reduce the number of firewall rules, simplifying network routes (or paths) — every Tempered Networks endpoint is just one hop away — and thereby reducing the amount of traffic that needs to be inspected by IDS/IPS and specialized threat analysis and protection devices. This saves precious cycles and reduces the potential for false positives.

Furthermore, in contrast to TCP, HIP was designed from its inception — through deployment of a cryptographic puzzle mechanism and a stateless-server approach toward key establishment and authentication — to be robust against the denial-of-service (DoS) and man-in-the-middle (MitM) attacks now plaguing the Internet.

Finally, there is the ability to quickly segment portions of the network and individual devices in order to limit the spread of malware or to quarantine an infected host. The notion of microsegmentation has become very popular as security professionals work to limit the exposure of data in the event of a breach. The Tempered IDN platform allows for easy and secure reconfiguration of network topology, enabling rapid response in the event of a breach and a malleable architecture that can adapt to changing business needs.

Challenges

While Tempered is taking an innovative approach to delivering an integrated solution that addresses problems that afflict networking and security, it faces a number of challenges in the marketplace.

First, Tempered's approach, based on HIP and cryptographic identity, is a departure from traditional networking and security tools based on TCP/IP. HIP represents a new path to secure and adaptable networks, and IT professionals will have to familiarize themselves with the technology before they become comfortable using it.

Although change in all facets of life is a constant, especially in IT, human beings (including IT professionals) are inclined to resist change, at least initially. IT practitioners will perceive all the risks associated with a new technology, but they will have a harder time perceiving the benefits or rewards that might accrue from using it. IT staff can be particularly skeptical when technologies are advertised as being easier to use and maintain. In these cases, IT personnel often instinctively assume that the claim is either exaggerated or that the ease of use is achieved through a trade-off in the product's overall effectiveness or performance.

Additionally, Tempered faces stiff and entrenched competition from established networking and security vendors. These vendors have large installed bases of customers and will be difficult to displace. Moreover, in the past few years, a number of security start-up companies have joined the fray, many of which claim to provide solutions in the realm of software-defined security. Amid such a crowded and competitive market, Tempered will have to ensure that it stands out from the crowd by clearly articulating its value proposition and creating sustainable differentiation.

Finally, as a start-up vendor itself, Tempered Networks must overcome customers' concerns about its long-term viability in the marketplace. In response, Tempered should cite the proven nature of its HIP-based technology and an engineering team that has grown sixfold since 2014.

Conclusion

IDC believes that the market imperative of digital transformation and the continued ascent of cloud computing are driving the need for a profound confluence of networking and security. While SDN has arisen as an architectural response to the networking requirements of cloud computing in the datacenter, and SD-WAN has emerged to address new connectivity requirements at branch offices and remote sites, there is an opportunity for a new variation of "secure SDN" to address connectivity and security challenges that span the entirety of the network.

Tempered Networks perceives this market need and has proposed its Identity-Defined Networking platform as a solution to the problem. With IDN, Tempered has acutely anticipated the secure networking requirements spawned by the pursuit of digital transformation and the robust growth of cloud computing. In enabling enterprise customers to secure network segments and to transform vulnerable IP-enabled devices into hardened, invisible assets, Tempered's IDN platform positions the company to address a market opportunity that will extend from the near-term needs of enterprise networks today to the long-term requirements associated with IoT well into the future**.**
